



Captain's Call

Don't Get Hooked By Phishers

According to the Federal Trade Commission (FTC), phishers are crooks who trick recipients into disclosing personal information such as Social Security numbers, passwords, bank account information and credit card numbers.

Phishing attacks come in e-mail form appearing to be from legitimate businesses. While the e-mails may seem like they're addressed directly to the recipient (as there is only one entry in the "To:" block), they are actually mass e-mailed to as many as a million addresses at a time.



The message tries to convince people that there is a problem with their account and the only way to fix it is to go to a special Web site where they can enter their account data. The site might look real, but it is run by scam artists who steal identities, run up bills and commit crimes in your name.

Such e-mails and Web sites even have familiar financial company logos, adding to the deception.

Additionally, phishers have mass e-mailed fake lottery-winning notifications which urge recipients to send their account information in order to transfer millions of dollars from foreign banks with the promise of giving the e-mail recipient a percentage of the account.

The FTC offers some tips to avoid being fooled:

- **Be suspicious** of all messages asking for personal or financial information.
- **Never send personal or financial information over e-mail**, including bank account numbers or passwords.
- **Regularly check credit card and bank statements.**
- **Free credit reports are online** (since Dec. 1), and can be requested at www.annualcreditreport.com from three nationwide consumer reporting agencies: Equifax, Experian, and TransUnion.
- **Keep antivirus and firewall software up to date.** Free antivirus software is available at the Space and Naval Warfare Systems Center (SPAWAR) site at <https://infosec.navy.mil>. Users must be on a ".mil" account to access the site, but the software can be downloaded and is authorized to be used on a home computer.

If you inadvertently submitted personal information, call FTC's ID-theft hotline at (877) ID-THEFT or file a report to FTC's Military Sentinel site at www.consumer.gov/military.

For related news, visit the Naval Network Warfare Command Navy NewsStand page at www.news.navy.mil/local/nnwc.